

DETAILED ACTION

This Examiner's Amendment and Examiner's Reasons for Allowance action is in response to the filing of 04/28/2009.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Shirley Lee Anderson (57,763) on 08/20/2009.

- The application has been amended as follows:

Claim 1 (Currently Amended) A method, performed by a computer processor executing computer executable instructions stored on a computer readable storage medium, of processing multiple types of security schemes, comprising:

receiving a message having a first token and a second token, wherein the first token and the second token are different from each other, while associated with a same subject;

extracting claims from one or more different types of security tokens corresponding to multiple security schemes, wherein each claim is a statement about each security token's subject that allows security schemes to be based on extracted claims;

authenticating the first token by extracting a first claim from the first token and authenticating the second token by extracting a second claim from the second token, wherein the first and second claims comprise different statements about the subject;

grouping the first and second claims into a claim collection by selectively mapping the first claim and the second claim to other claims;

determining a resource being accessed by extracting or obtaining resource identifiers from [[a]] the message at run-time or examining a static configuration of a service;

authorizing access to [[a]] the resource referred to in the message based at least in part on the first and second claims; [[and]]

supporting multiple security schemes for the method; and
the resource corresponds to at least one of the resource identifiers stored by a computing system.

[Claims 2-3 are entered as they are without any changes].

Claims 5 & 6 (Cancelled).

Claim 7 (Currently Amended) The method of claim [[6]] 1, wherein obtaining the resource from the message comprises applying an XPath expression.

Claim 8 (Currently Amended) The method of claim [[6]] 1, wherein the resource identifier comprises a property of the message.

Claim 9 (Cancelled).

Claim 10 (Currently Amended) The method of claim [[6]] 1, wherein the resource identifier comprises a property of the computing system's runtime environment.

Claim 11 (Cancelled).

[Claims 12-18 are entered as they are without any changes].

Claim 19 (Cancelled).

Claim 20 (Currently Amended) A system configured to process multiple types of security schemes, the system comprising,

one or more computer processors; and

one or more computer readable storage media, storing computer executable instructions that are executable by the one or more computer processors, ~~to store~~ the computer executable instructions comprising:

a first module to extract claims from one or more different types of security tokens corresponding to multiple security schemes, wherein [[a]] each claim is a statement about [[a]] each security token's subject that allows security schemes to be based on the extracted claims;

the first module authenticates by [[to]] extracting a first claim from a first token and a second claim from a second token associated with a message, wherein the message has an associated subject and the first claim and the second claim comprise different statements related to the subject;

a second module to selectively map the first claim and the second claim to other claims;

the second module to determine a resource being accessed by extracting or obtaining resource identifiers from [[a]] the message at run-time; [[and]]

the second module to authorize access to the resource referred to in the message based at least in part on the first and second claims;

the first module and the second module form a claim collection that includes the first and second claims;

the first module and the second module supporting multiple security schemes; and
the resource corresponds to at least one of the resource identifiers stored by a computing
system.

[Claims 21 & 22 are entered as they are without any changes].

Claims 23 & 24 (Cancelled).

Claim 25 (Currently Amended) The system of claim [[24]] 20, wherein the module to obtain the resource identifier from the message is to selectively apply an XPath expression to obtain the resource identifier.

Claim 26 (Currently Amended) The system of claim [[24]] 20, wherein the resource identifier comprises a property of the message.

[Claims 27 & 28 are entered as they are without any changes].

Claim 29 (Cancelled).

[Claims 30-36 are entered as they are without any changes].

Claim 37 (Cancelled).

Claim 38 (Currently Amended) A computer-readable storage medium storing computer-executable instructions that, executed by a processor, perform[[s]] acts comprising:

receiving a message having a first token and a second token, wherein the first token and the second token are different from each other, but associated with a same subject;

extracting claims from one or more different types of security tokens corresponding to multiple security schemes, wherein [[a]] each claim is a statement about [[a]] each security token's subject that allows security schemes to be based on the extracted claims;

authenticating by obtaining a first claim from the first token and a second claim from the second token, wherein the first and second claims comprise different statements about the subject;

grouping the first and second claims into a claim collection by selectively mapping the first claim and the second claim to other claims; [[and]]

determining a resource being accessed by extracting or obtaining resource identifiers from the message at run-time or examining a static configuration of a service;

authorizing access to the resource referred to in the message based at least in part on the first and second claims;

supporting multiple security schemes for the acts; and

the resource corresponds to at least one of the resource identifiers stored by a computing system.

[Claims 39-48 are entered as they are without any changes].

Allowance

2. Claims 5, 6, 9, 11, 19, 23, 24, 29, & 37 have been cancelled.
3. Claims 1-4, 7, 8, 10, 12-18, 20-22, 25-28, 30-36, & 38-48 have been amended with written arguments which overcome the examiner's prior rejections and objections, see paper of 7/21/05. Examiner withdraws all outstanding rejections and objections to Claims 1-4, 7, 8, 10, 12-18, 20-22, 25-28, 30-36, & 38-48.
4. Claims 1-4, 7, 8, 10, 12-18, 20-22, 25-28, 30-36, & 38-48 are allowed.

Examiner's Statement of Reasons for Allowance

5. Prior art was found which disclosed [e.g. Janis (5,263,158)].
6. The following is an examiner's statement of reasons for allowance:
 - The prior art of record does not teach or render obvious the limitations as recited in independent Claims 1, 20, & 38 specific to "extracting claims from one or more different types of security tokens corresponding to multiple security schemes" and "a claim is a statement about a security token's subject that allows security schemes to be based on extracted claims" and "grouping the first and second claims into a claim collection by selectively mapping the first claim and the second claim to other claims" and "determining a resource being accessed by extracting or obtaining resource identifiers from a message at run-time or examining a static configuration of a service" and "authorizing access to a resource referred to in the message based at least in part on the first and second claims" and "supporting multiple security schemes for the method".
 - Dependent claims are allowed as they depend from an allowable independent claim.
 - Therefore, the Examiner considers the combination of the above claim limitations and the remaining limitations of each independent claim as applied to security claim processing which supports multiple security schemes as the non-obvious novelties of the invention.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OSCAR A LOUIE/
08/20/2009

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436